

# Notice of Allowability

Application No.

09/637,229

Examiner

Christian La Forgia

Applicant(s)

KOC ET AL.

Art Unit

2131

## -- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 14 December 2006.
2. ☒ The allowed claim(s) is/are 6,7,9-11,16,18 and 22-29.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) ☐ All    b) ☐ Some\*    c) ☐ None    of the:
  1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

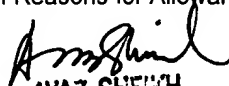
\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.  
**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.
  - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review ( PTO-948) attached
    - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
  - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

### Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08),  
Paper No./Mail Date \_\_\_\_\_
4. ☐ Examiner's Comment Regarding Requirement for Deposit  
of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413),  
Paper No./Mail Date mail'd with action.
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other \_\_\_\_\_

  
**AYAZ SHEKH**  
**SUPERVISORY PATENT EXAMINER**  
**TECHNOLOGY CENTER 2100**

### EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

2. Authorization for this examiner's amendment was given in a telephone interview with Michael Jones (Reg. No. 41,879) on 22 February 2007.

3. The application has been amended as follows:

In the Claims

16. (Currently Amended) A method of determining a Montgomery product of a first cryptographic parameter and a second cryptographic parameter, the method comprising:

representing the first cryptographic parameter as a series of bits;

representing the second cryptographic parameter and a modulus as a series of words;

processing a first bit of the first parameter with each word of the modulus and each word of the second parameter to produce a first series of intermediate values and a contribution to the Montgomery product based on the first bit;

processing a second bit of the first parameter with each word of the modulus and each word of the second parameter, and a corresponding intermediate value from the first series of intermediate values to produce a second series of intermediate values and a contribution to the Montgomery product based on the second bit, wherein the first series of intermediate values and the second series of intermediate values are determined based on a field-type input that selects an arithmetic operation to be performed in accordance with  $GF(p)$  or  $GF(2^m)$  arithmetic, wherein

Art Unit: 2131

$GF(p)$  is a prime field,  $GF(2^m)$  is a binary extension field,  $p$  is a positive prime number, and  $m$  is a positive integer, ~~and~~

combining the first contribution and the second contribution; and

using the combination of the first and second contributions in a cryptographic process.

#### **DETAILED ACTION**

4. The amendment of 14 December 2006 has been noted and made of record.
5. Claims 6, 7, 9-11, 16, 18, and 22-29 have been presented for examination.
6. Claims 1-5, 8, 12-15, and 19-21 have been cancelled as per Applicant's request.

#### ***Response to Arguments***

7. Applicant's arguments, see page 6, filed 14 December 2006, with respect to the 35 U.S.C. 112, 2<sup>ND</sup> paragraph rejection of claim 22 have been fully considered and are persuasive. The rejection of claim 22 has been withdrawn.
8. Applicant's arguments, see pages 7 and 8, filed 14 December 2006, with respect to the rejection of independent claims 6 and 16 have been fully considered and are persuasive. The rejection of claims 6, 7, 9-11, 16, 18, and 22-29 has been withdrawn.

#### ***Allowable Subject Matter***

9. Claims 6, 7, 9-11, 16, 18, and 22-29 are allowed.
10. The following is an examiner's statement of reasons for allowance:

As per claims 6 and 16, the record has shown that there are several well-known techniques for computing Montgomery products.

The record also shows that the prior art is lacking in a field-type input that selects between the  $GF(p)$  prime and  $GF(2^m)$  binary extension fields. Since no teachings or motivation

Art Unit: 2131

can be found a of field-type input that selects between the GF(p) prime and GF( $2^m$ ) binary extension fields, claims 6, 7, 9-11, 16, 18, and 22-29 are therefore novel and non-obvious.

11. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

### *Conclusion*

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

13. The following patents are cited to further show the state of the art with respect to Montgomery multipliers, such as:

United States Patent No. 6,925,563 to Jennings, which is cited to show modular multiplication using the Montgomery algorithm.

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

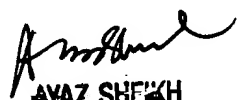
15. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

16. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia  
Patent Examiner  
Art Unit 2131

clf

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100